STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD** P800-S895 Rev 1.0	**TITLE: Security Training and Awareness** Effective Date: April 5, 2004

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to define criteria for a security training and awareness program at State budget units designed to educate State employees of the requirements to protect State information and IT resources and provide the knowledge and skills necessary to fulfill IT security responsibilities for the State.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Policies (PSPs) within each budget unit.

4. STANDARD

The following standards provide criteria for budget unit security awareness and training programs to clearly outline State employee responsibilities.

4.1. CONTENT: Security awareness training content shall be created and regularly reviewed, and updated, on a frequency determined and documented by the budget unit, to ensure that it addresses the budget unit's organizational mission, culture, business, technology, systems, and data/information.

4.1.1. Training material shall include, at a minimum, content that:

- Enables the individual to understand the meaning of IT security, why it is needed, and his/her personal responsibility for security along with the importance of complying with all Statewide and budget-unit-specific security policies and standards.
- Includes or references *Statewide Policy P800, IT Security*, Statewide security standards, and Statewide policies for email and Internet use that establish basic, general rules of employee

behavior. Budget units should elaborate as necessary to adapt these basic, general rules of behavior into their own culture based on business services and requirements, to reduce the possibility for confusion or misunderstanding. Where budget unit IT security requirements are more stringent than Statewide IT security policies and standards, those elements should be clearly explained.

- Enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to budget unit data/information and IT resources.
- Enables the individual to better understand social engineering persuasion techniques that may be used to deceive an individual into revealing confidential, private, or privileged information in order to compromise the confidentiality, integrity, and availability of budget unit data/information and IT resources.
- Includes technical alternatives, methods, and standards which represent best practices appropriate to budget unit data/information and IT resources, and which can be utilized to effectively implement safeguards, as appropriate.
- Covers, but is not limited to
    - The responsibility of individuals to report IT-security-related issues;
    - The fact that an individual's activities can be audited;
    - The legal requirements for data (citing legislation as appropriate);
    - Privacy expectations of State employees and third-party organizations;
    - The ownership of data;
    - Non-business use issues;
    - The budget unit's password requirements for usage and management;
    - Virus and malicious code protection;
    - Incident response procedures;
    - The budget unit's acceptable use policy for email and Internet Use;
    - Encryption technologies and the transmission of sensitive/confidential information over the Internet;
    - The budget unit's intellectual property and fair use requirements;
    - Supported/allowed software on budget unit systems;
    - The sensitivity of budget unit systems to threats, risks, and vulnerabilities;
    - Social engineering techniques commonly used to deceive users into giving away access or revealing confidential or privileged information;
    - Physical security; and
    - Applicability of security requirements to all IT resources, including portable IT devices, such as laptops, etc.

4.1.2. Security awareness training materials (manuals, documents, etc.) as well as IT security policies, standards, and procedures should be made readily available, either electronically or via hard copy, to all State employees.

4.1.3. Budget units should incorporate formal evaluation and feedback mechanisms to gauge the appropriateness and effectiveness of its security awareness and training programs, techniques, and materials.

4.2. ROLES AND RESPONSIBILITIES: Budget units should clearly define and document key personnel IT security roles and responsibilities. Contact information, as appropriate, should be included in security awareness and training manuals, documents, handouts, etc.

4.3. LEVEL OF AWARENESS AND TRAINING: The level of security awareness and training should be commensurate with the level of access and expertise required in relation to the system components and information resources for which the State employee is responsible.

- Security awareness and training should be incorporated into a budget unit's new hire training for every State employee.
- All State employees should receive security training prior to being provided any access to IT systems and resources. Prior to accessing State or budget unit specific software applications, employees should receive any specialized security training as appropriate focused for their role and responsibility relative to the software application system.
- The receipt of security awareness training should be documented in the employee's personnel file with the employee's acknowledgement of having received and understood the training.
- Security awareness shall be promoted on an on-going basis. State employees should have their security awareness training updated annually or upon occurrence of a specific event, such as a change in job responsibilities, employment status, etc.

4.4. LEVERAGE OF KNOWLEDGE: Budget units are encouraged to share their security awareness training programs and materials with other budget units.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))), "State Agency Information."
6.3. A. R. S. § 41-1339 (A), "Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."

6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P252, Intellectual Property and Fair Use.
6.17. Statewide Policy P401, Email Use.
6.18. Statewide Policy P501, Internet Use.
6.19. Statewide Policy P800, IT Security.
- 6.18.1. Statewide Standard P800-S805, IT Risk Management.
- 6.18.2. Statewide Standard P800-S810, Account Management.
- 6.18.3. Statewide Standard P800-S815, Configuration Management.
- 6.18.4. Statewide Standard P800-S820, Authentication and Directory Services.
- 6.18.5. Statewide Standard P800-S825, Session Controls.
- 6.18.6. Statewide Standard P800-S830, Network Security.
- 6.18.7. Statewide Standard P800-S850, Encryption Technologies.
- 6.18.8. Statewide Standard P800-S855, Incident Response and Reporting.
- 6.18.9. Statewide Standard P800-S860, Virus and Malicious Code Protection.
- 6.18.10. Statewide Standard P800-S865. Business Continuity/Disaster Recovery Plan (BCDR).
- 6.18.11. Statewide Standard P800-S870, Backups.
- 6.18.12. Statewide Standard P800-S875, Maintenance.
- 6.18.13. Statewide Standard P800-S880, Media Sanitizing/Disposal.
- 6.18.14. Statewide Standard P800-S885, IT Physical Security.
- 6.18.15. Statewide Standard P800-S890, Personnel Security.

6.20. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.